

Notice of Allowability

Application No.

09/932,547

Examiner

Minh Dinh

Applicant(s)

KAPLAN, JONATHAN C.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to a telephone interview given on 3/16/2005.
2. ☒ The allowed claim(s) is/are 1-10, 12-26, 28-31, 33 and 34.
3. ☒ The drawings filed on 17 August 2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 1/7/02 and 4/11/02
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

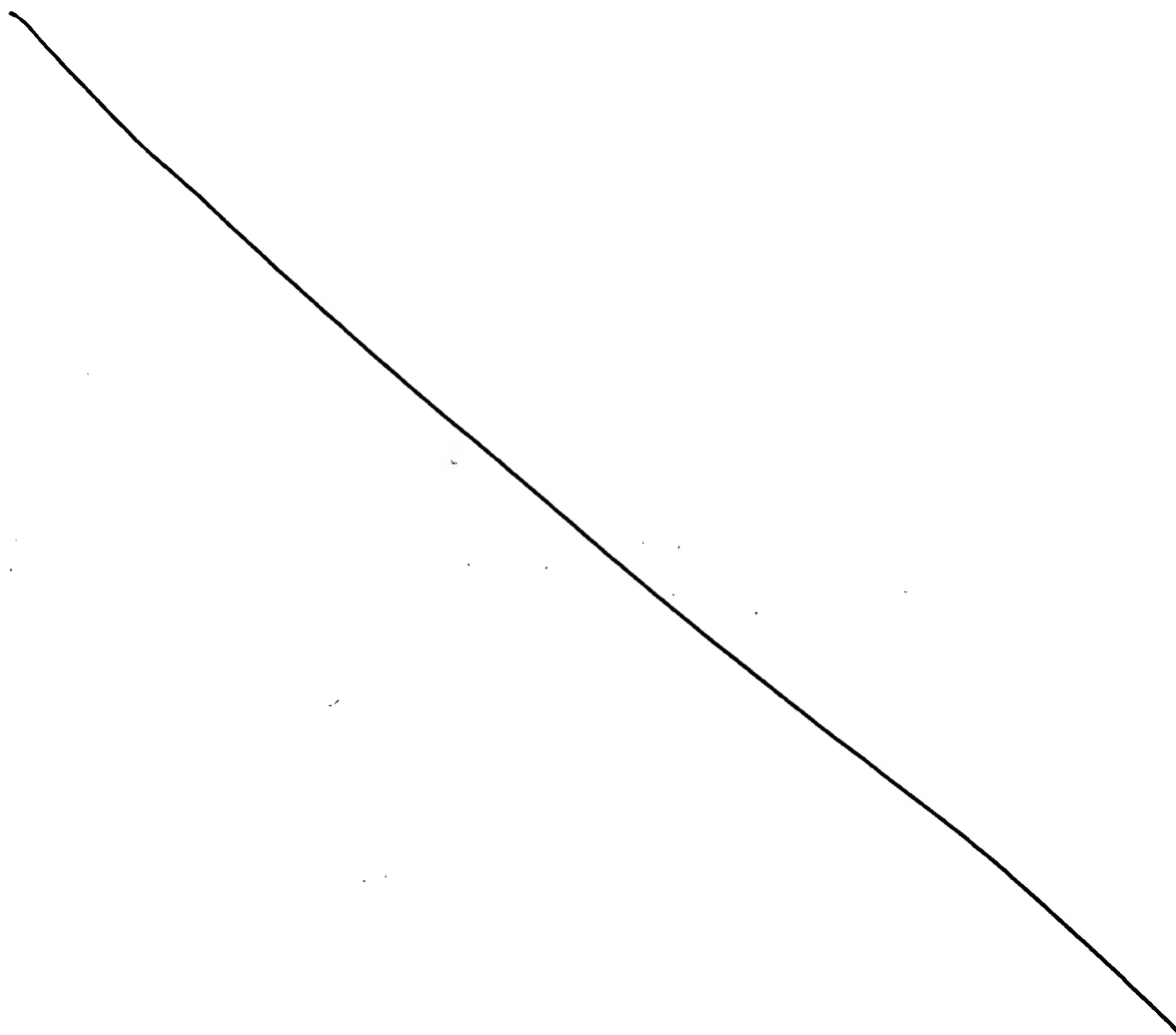
Art Unit: 2132

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Victor Johnson on 3/16/2005.

The application has been amended as follows: claims 1, 15, 31 and 33-34 have been amended; claims 11, 27, 32 and 35-36 have been cancelled.



Art Unit: 2132

1. (Currently amended) A method to verify authenticity of a document having an electronic signature associated therewith, said document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, the method comprising the following steps:

(a) creating a document identification number (DID) uniquely associated with said DFP, and associating said DID with said DFP;

(b) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP; and

(c) storing, in at least ~~[[one location]]~~ two locations, registration certificate ~~[[information]]~~ (DFC) that represents said electronic signature and includes said DID, said DFP, and said C, such that a single entity cannot modify every stored copy of said DFC;

wherein step (c) includes initially promulgating said DFC to at least a minimum number Q of N, where $N > Q$, storage locations (WS), and subsequently promulgating said DFP to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC;

wherein authenticating whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

comparing a putative digital fingerprint ~~[[DFP']]~~ DFP' for said DF' obtained using said CHF with at least ~~[[one]]~~ two retrieved ~~[[copy]]~~ copies of said DFP associated with the DFC stored at step (c);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

2. (Original) The method of claim 1, wherein at step (b), said credential information (C) is obtained from a user-registrant who initiates said association of said DID with said DFP.

3. (Original) The method of claim 1, wherein at step (a), said credential information (C) includes at least one type of information selected from a group consisting of (i) user-registrant identity, (ii) user-registrant password, (iii) user-registrant provided authenticating information from a two-factor authentication device, (iv) user-registrant cryptographic key information, (v) user-registrant client system identifier, and (vi) user-registrant provided authenticating hardware token information.

4. (Original) The method of claim 1, wherein at step (a), said association of said DID with said DFP is initiated by a user-registrant, said user-registrant selecting an archive-server in which said DF and at least DFC information will be stored.

5. (Original) The method of claim 1, further including storing said DF and at least DFC information in an archive-server, said archive-server verifying authenticity of said DF and said at least DFC information stored therein.

6. (Original) The method of claim 1, wherein step (a) includes selecting a document identification number (DID) at least quasi-randomly.

7. (Original) The method of claim 1, wherein step (a) includes generating said document identification number (DID) by a nexus-server.

8. (Original) The method of claim 1, wherein said DFP is representable in at least one format selected from a group consisting of (i) a printable bar-code, (ii) a

printable multi-dimensional bar-code, (iii) printed scannable information, (iv) scannable information, and (v) human-readable information.

9. (Original) The method of claim 1, wherein step (c) includes selecting locations for said storage at least quasi-randomly.

10. (Original) The method of claim 1, wherein said document is protectable by copyright law, and said method is carried out at least in part to protect a copyright for said document, wherein said copyright law is selected from a group consisting of (i) U.S. copyright law, and (ii) copyright law of nations other than the U.S..

11. (Cancelled, without prejudice or disclaimer)

12. (Original) The method of claim 11, wherein step (c) includes initially promulgating said DFC substantially in real-time.

13. (Original) The method of claim 11, wherein:
each of said Q storage locations independently determines and independently reports a timestamp including time of its receipt of said DFP; and
said DFC stored at step (c) includes at least each independently reported said timestamp.

14. (Original) The method of claim 13, further including:
comparing time reported from each said timestamp to determine from a commonality thereof that time at which storing at step (c) occurred is not disputable.

15. (Currently amended) A method to verify authenticity of a document having an electronic signature associated therewith, said document being digitally

representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, the method comprising the following steps:

- (a) creating a document identification number (DID) uniquely associated with said DFP, and associating said DID with said DFP;
- (b) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP;
- (c) creating a signature declaration (SD) that captures expressed intent of a user-registrant to create and associate said electronic signature with said document represented by said DF;
- (d) creating a testimonial record (T) that includes at least said DID, said DFP, said C, and said SD, and creating from and associating with said T a unique digital fingerprint number (DFP_T), said DFP_T obtainable from a cryptographic hash function (CHF_T); and
- (e) storing, in at least ~~[[one location]]~~ two locations, registration certificate ~~[[information]]~~ (DFC_T) that represents said electronic signature and includes said DID, said DFP, said DFP_T, and said C, such that a single entity cannot modify every stored copy of said DFC_T;

wherein wherein step (e) includes initially promulgating said DFC to at least a minimum number Q of N, where $N > Q$, storage locations (WS), and subsequently promulgating said DFP to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC;

wherein authenticating whether a putative document, digitally representable as a putative file DF' and associated with a putative registration certificate (DFC_T') and associated with a putative testimonial record (T'), is an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

comparing a putative digital fingerprint DFP' for said DF' obtained using said CHF with at least ~~[[one]]~~ two retrieved ~~[[copy]]~~ copies of said DFP associated with the DFC_T stored at step (e), and

comparing a putative digital fingerprint DFP_T' for said T' obtained using said CHF_T with at least ~~[[one-copy]]~~ two copies of said DFP_T associated with the DFC_T stored at step (e);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and if said DFP_T' and said DFP_T are in agreement, said electronic signature has not been altered.

16. (Original) The method of claim 15, wherein said DF includes a DFC_T previously stored at step (e).

17. (Original) The method of claim 15, further returning to said user-registrant information that includes at least said T and said DFP_T.

18. (Original) The method of claim 15, further including storing within a system-of-record information that includes at least said T.

19. (Original) The method of claim 15, wherein step (b) is carried out by a system-of-record that stores information including at least said T.

20. (Original) The method of claim 15, wherein at step (b), said credential information (C) is obtained from a user-registrant who initiates said association of said DID with said DFP.

21. (Original) The method of claim 15, wherein at step (b), said credential information (C) includes at least one type of information selected from a group

consisting of (i) user-registrant identity, (ii) user-registrant password, (iii) user-registrant two-factor authentication, and (iv) user-registrant key information.

22. (Original) The method of claim 15, wherein at step (a), said association of said DID with said DFP is initiated by a user-registrant, said user-registrant selecting an archive-server in which said DF and at least DFC information will be stored.

23. (Original) The method of claim 15, further including storing said DF and at least DFC information in an archive-server, said archive-server verifying authenticity of said DF and said at least DFC information stored therein.

24. (Original) The method of claim 15, wherein step (a) includes selecting a document identification number (DID) at least quasi-randomly.

25. (Original) The method of claim 15, wherein step (a) includes generating said document identification number (DID) by a nexus-server.

26. (Original) The method of claim 15, wherein step (e) includes selecting locations for said storage at least quasi-randomly.

27. (Cancelled without prejudice or disclaimer)

28. (Original) The method of claim 27, wherein step (e) includes initially promulgating said DFC substantially in real-time.

29. (Original) The method of claim 27, wherein:
each of said Q storage locations independently determines and independently reports a timestamp including time of its receipt of said DFP; and

said DFC stored at step (e) includes at least each independently reported said timestamp.

30. (Original) The method of claim 29, further including:
comparing time reported from each said timestamp to determine from a commonality thereof that time at which storing at step (c) occurred is not disputable.

31. (Currently amended) A method to verify authenticity of a document optionally having an electronic signature associated therewith, said document being digitally representable as a file (DF) processable with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, where (i) a document identification number (DID) uniquely associated with said DFP has been created and associated with said DFP; where (ii) credential information (C) has been obtained, its veracity confirmed, and said C associated with said DID and said DFP; and (iii) where there has been stored in at least ~~[[one location]]~~ two locations registration certificate ~~[[information]]~~ (DFC) representing said electronic signature and including said DID, said DFP, and said C, such that a single entity cannot modify every stored copy of said DFC wherein said DFC has been promulgated to at least a minimum number Q of N, where $N > Q$, storage locations (WS), and has subsequently been promulgated to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC; the method comprising the following steps:

(a) for a putative document, obtaining a digital representation thereof as a putative file DF' and obtaining a putative registration certificate (DFC') associated therewith;

(b) obtaining and comparing a putative digital fingerprint ~~[[DFP]]~~ DFP' for said DF' obtained using said CHF with at least ~~[[one]]~~ two retrieved ~~[[copy]]~~ copies of said DFP associated with said DFC;

wherein said putative document is an unaltered version of said document represented by said DF and is associated with said electronic signature; and includes:
if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

32. (Cancelled, without prejudice or disclaimer)

33. (Currently amended) A system to verify authenticity of a document representable digitally, the system comprising:

a nexus-server having a CPU and memory and including means for quasi-randomly generating ID numbers, issuing customer ID numbers, issuing document ID numbers (DID), and issuing coupons bearing at least one of (i) CID, and (ii) DID;

at least ~~[[one cluster]]~~ two clusters of witness-server computer systems (WS), each having a CPU and memory, each of said witness-servers being operatively coupleable to each other and to said nexus-server for intercommunication therebetween;

wherein said nexus-server supervises adherence of said WS in a cluster to rules and protocols applicable to said cluster;

wherein ~~[[at least one of said]]~~ one WS of said cluster, upon presentation by a user of said coupon and a digital fingerprint number (DFP) for said document obtained from a one-way cryptographic hash function (CHF), promulgates said coupon information and said DFP to ~~[[at least a minimum]]~~ a number of other ~~[[of said]]~~ witness-server computer systems in said cluster, wherein said number of other witness-server computer systems is at least two and is commensurate with the value of the coupon, and upon confirming receipt of said coupon information and said DFP, ~~[[from said minimum number, said one of]]~~ said witness-server computer ~~[[systems]]~~ system converting said coupon into a registration certificate containing at least said coupon information and said DFP, said registration certificate is returned to said user;

said system upon user-presentation of said registration certificate retrieving from at least some of said witness-server computer systems in said cluster a digital fingerprint number;

wherein comparison of the retrieved said digital fingerprint numbers against a digital fingerprint number newly generated for said document permits confirming said document has was not altered after presentation to said system.

34. (Currently amended) ~~[[Media]]~~ A computer-readable medium storing computer-readable software that when executed by a computer system that includes a CPU carries out at least three of the following steps to verify authenticity of a document having an electronic signature associated therewith, the document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF:

(a) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP;

(b) creating a signature declaration (SD) capturing expressed intent of a user-registrant to create and associate said electronic signature with said document;

(c) promulgating for storage, in at least ~~[[one location]]~~ two locations, registration certificate ~~[[information]]~~ (DFC) that represents said electronic signature and includes said DID, said DFP, said C, and at least one of (i) said SD, and (ii) a digital fingerprint of said SD, such that a single entity cannot modify every stored copy of said DFC;

wherein step (c) includes initially promulgating said DFC to at least a minimum number Q of N, where $N > Q$, storage locations (WS), and subsequently promulgating said DFP to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC;

wherein authenticating whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is

an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

(d) comparing a putative digital fingerprint ~~[[DFP']]~~ DFP' for said DF' obtained using said CHF with at least ~~[[one]]~~ two retrieved ~~[[copy]]~~ copies of said DFP associated with the DFC stored at step (c);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

35-36. (Cancelled, without prejudice or disclaimer)

Art Unit: 2132

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and system for registering a document and using a registration certificate stored at a server to verify the authenticity of a document. More specifically, independent claims 1, 15, 31 and 34 identify the uniquely distinct features of storing, in at least two locations, registration certificate (DFC) including the hash of the document wherein storing includes initially promulgating the DFC to at least a minimum number Q of N , where $N > Q$, storage locations, and subsequently promulgating the DFC to any remaining $(N-Q)$ said storage locations not initially receiving promulgated DFC. The closest prior art, Haber et al (5,136,647), discloses a method for authenticating a document using a certificate including the step of sending certificate information including the hash of the document to a number of witness servers. However, Haber does not teach initially promulgating said certificate to at least a minimum number Q of N , where $N > Q$, storage locations, and subsequently promulgating said certificate to any remaining $(N-Q)$ said storage locations not initially receiving promulgated said certificate.

Independent claim 33 identifies the uniquely distinct features promulgating coupon information including a user ID or a document ID and a hash value of a document to a number of witness servers, the number of witness servers being commensurate with the value of the coupon, and converting said coupon into a certificate after receiving confirmation from the witness servers. The closest prior art, Haber et al (5,136,647), discloses a method for authenticating a document using a certificate including the step of sending information including a user ID and a hash of a

Art Unit: 2132

document to a number of witness servers. Another prior art, Weiant, Jr. et al (6,044,350) teaches that service charge for a requested service is commensurate with a security level selected by a user. However, Haber and Weiant, Jr. do not disclose that the number of witness servers is commensurate with service charge.

The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claims, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

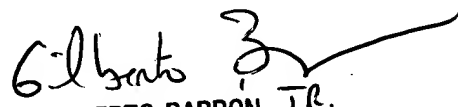
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
3/17/05


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100